FORTUNE

Hacking Coinbase: The Great Bitcoin Bank Robbery

By **JEN WIECZNER** August 22, 2017

Sean Everett wasn't sure how his bullish bet on cryptocurrency would turn out. But he definitely didn't expect it to be over so soon.

In March, he sold all his stocks, including Apple and Amazon, and used a chunk of the proceeds to buy Bitcoin and Ethereum on a site called Coinbase. The decision made Everett, the CEO of artificial intelligence startup Prome, almost instantly richer, as the blockchain-based currencies' value rocketed up exponentially over the next several weeks. But then, while he was out walking the dog after 10 p.m. on Wednesday, May 17, Everett got the call. It was T-Mobile, ringing him to confirm that it was switching his phone number to a different device.

It was a suspicious move that Everett had most certainly not requested. But even as he pleaded with the agent to block the switch, it was too late. Less than five minutes later, Everett's cell service abruptly shut off, and as he rushed to his computer, he saw himself being robbed in real time. A raft of email notifications confirmed that someone had taken control of his main Gmail account, then broken into his Coinbase "wallet." They'd gotten in with the help of his switched-over phone number: Everett's account required him to log in with a two-factor authentication code sent by text message, as a second safeguard—and now the text had gone straight to the thief.

It took only two minutes for the attacker to clean Everett out of what was then a few thousand dollars' worth of digital coins. From Everett's perspective, the even more painful heist was what came next: Ethereum's price quadrupled over the next three weeks. It had reached its all-time high of $400 just hours before I met Everett in a New York coffee shop on a humid June afternoon. Bitcoin, meanwhile, had broken $3,000 for the first time a day earlier, and Everett was pining for his missing digital

coins. "I'm not only still out my money, I also didn't get the rise in price," he lamented.

Then again, the biggest surprise for Everett—and, it would turn out, for many other Bitcoin enthusiasts—was that the theft happened on Coinbase at all. San Francisco's Coinbase, the world's largest exchange for trading cryptocurrency, is one of very few such companies whose own coffers have never been hacked, a distinction that carries extra weight in the realm of blockchain, where several costly breaches have made global headlines. Almost any early investor you talk to lost money in Mt. Gox, an exchange that collapsed in 2014 after hackers pillaged nearly $500 million in Bitcoin. Last summer, thieves grabbed $72 million from Hong Kong cryptoexchange Bitfinex in one fell swoop.

But hackers have never breached Coinbase's own virtual fortress, and that impenetrability has earned it a reputation as the safest place to buy Bitcoin, helping it attract more than 9 million customers who store at least $3 billion in crypto-currency there, and who have traded $25 billion to date on its retail brokerage as well as its institutional exchange, GDAX. The five-year-old Coinbase just raised $100 million in new funding, valuing the company at $1.6 billion—making it the blockchain industry's first "unicorn." "If you look at what they are world-class at, it's security, trust, safety ... all these things that, frankly, banks are good at," Fred Wilson, the venture capitalist and one of Coinbase's earliest and largest backers, said at a conference in March. "They're like JPMorgan or Goldman Sachs for blockchain."

But Coinbase's individual customers do get burglarized—with surprising and unsettling frequency. Even Wilson himself was in for a rude awakening: While vacationing in Europe in early June, the VC woke up to the same telltale emails that Everett saw, signaling that an intruder was trying to get inside his Coinbase account. Wilson managed to lock it down before anything was stolen, but in a rare public chastising of a company in his own portfolio, he wrote in a blog post: "I am still a bit shaken up from the experience and a fair bit more paranoid from it."

Since then, *Fortune* has spoken with more than a dozen victims, including tech CEOs and well-known blockchain proponents, whose Coinbase accounts have been targeted and hacked in almost exactly the same fashion; still more have been

attacked on other exchanges. The day after Everett's robbery, Los Angeles entrepreneur Adam Dachis's account was wiped out of what was then $10,000. On July 7, thieves emptied $18,000 from the Coinbase wallet of blockchain adviser Mike Costache, during the four hours he slept one night while traveling overseas. Since Christmas, there have been months when Coinbase users have been robbed as often as 30 times—a rate of one robbery every single day.

In each case, the same blindsiding realization arrives, bringing the inherent paradox of blockchain into focus. The quintessential strength that sets cryptocurrency apart from traditional money—that transactions are instant and irreversible—is also its fatal flaw. "One of [Bitcoin's] reasons for existence is that it's censorship-resistant," says Tom Robinson, cofounder and chief data officer of Elliptic, a London-based blockchain intelligence firm. That means no one, not even a government or central bank, can stop a digital currency transaction from happening. And therefore the fraud protections traditional bank depositors rely on are mostly unavailable. "Any kind of charge-back and reversibility would be the antithesis of what Bitcoin was created to achieve," says Robinson.

That's one reason that, when criminals want to pull a heist, they're increasingly choosing cryptocurrency over real dollars. In 2016, $28 million in losses from crimes involving virtual currency were reported to the FBI's Internet Crime Complaint Center, more than triple the 2015 total. And that figure is based heavily on voluntary reports by individual victims. It doesn't include large-scale thefts from exchanges like the Bitfinex hack, so it likely underestimates the true damages by many orders of magnitude.

Cybercrime is rising at traditional financial institutions too: For example, thefts through so-called account takeovers, a crime analogous to the Coinbase hacks, rose 61% last year to $2.3 billion, according to Javelin Strategy & Research. But hacking losses are a blip relative to the trillions of dollars kept in banks. Hackers are stealing a much larger proportion of the cryptocurrency pie, whose total market value is only about $135 billion. In the past 12 months, for example, criminals have absconded with 1% of Ethereum's total market value, or $225 million, according to cybersecurity firm Chainalysis; the Bitcoin toll is estimated to be even higher.

Brick and mortar bank robbers have "two problems: stealing the money and hiding the evidence," explains Moran Cerf, a professor of business and neuroscience at Northwestern's Kellogg School of Management and a former corporate hacker. "Bitcoin solves the second one for you because everyone there is anonymous." Bitcoin diehards seem resigned to the reality of irreversible transactions—and its drawbacks. "I think of that as a feature and not a bug," says Chris Burniske, a blockchain investor and author of forthcoming book *Cryptoassets*—even though his own accounts were looted in December for digital coins that would now be worth over $100,000.

But when victims watch their money up and leave into the digital wallet of a nameless stranger, it becomes more than just a problem for Coinbase: It's a threat to the promise of Bitcoin itself. As the value of cryptocurrency soars, more investors are grappling not just with how to profit from it, but how to hold on to it at all. "Coinbase looks like a bank, talks like a bank, and takes millions of dollars in cash like a bank, but, in practice, it functions like a dimly lit underground casino," says Cody Brown, whose account was hacked for $8,000 in the span of just 15 minutes in May. "You don't realize that the balanced fonts, smooth blue gradients, and endless copy about trust mean absolutely nothing—until you are robbed blind."

See also: Blockchain Mania: Why Big Business Is Racing to Build Blockchains

Coinbase, for its part, won't discuss specific cases except to say that it investigates all account takeovers. But Brian Armstrong, Coinbase's 34-year-old CEO and founder, says Brown's and Wilson's experiences were "helpful" in teaching the company how to improve. Its security measures already match or exceed those at banks—from using machine learning to detect dubious activity, to mandating dual-factor authentication. Yet Armstrong recognizes that Coinbase is also a juicier target: "We need to be held to a higher standard," he tells *Fortune*, "because digital currency is so new and interesting and powerful that it is attractive to a lot of people out there to try to steal it."

If Bitcoin were a religion, its equivalent of "What would Jesus do?" would be "BYOB: Be your own bank," an unofficial slogan widely embraced in the industry. The original blockchain was launched in 2009, by the mysterious founder (or founders)

going by the name Satoshi Nakamoto, as a utopian form of electronic cash that could change hands, as Nakamoto wrote in a legendary white paper, "without going through a financial institution."

But that ideal also attracted a subversive element, repelling many potential adopters. That's where Armstrong saw an opportunity to bring polish to an industry run by "hackers and cryptoanarchists" at the time, he says: "If this was going to go mainstream, it needed something that had a more trusted brand around it."

An early engineer at Airbnb, Armstrong quit in 2012 to create the "Gmail for digital currency." His strategy: making it easier and safer to store, and then buy and sell, cryptocurrency. While early Bitcoin wallet companies made people keep track of their own private keys—the secret 64-character passwords that alone provide access to one's cryptocurrency—Coinbase's pioneering innovation was its offer to store keys on customers' behalf. That also came with risk, as customers wouldn't need to know their actual key, but rather just a password, to get to their Bitcoins—and neither would a hacker. "That's a big responsibility to take on," the fresh-faced CEO admits. "But I also think it's necessary to help the industry scale and make digital currency accessible to the next 100 million or billion people."

Coinbase has demonstrated a unique ability to bring the new asset class to the masses. Its base of customers, most of whom are in the U.S., has grown 50% just in the past five months, with as many as 50,000 signing up in one day; trade volume in July alone was twice as much as all last year. Coinbase, which makes money by charging transaction fees, is said to be nearing profitability, and Armstrong ranks No. 10 on this year's *Fortune* 40 Under 40 list. But he is pretty clear about his company's limits. "The average person may at a high level think of us as a digital currency bank, but we're not a bank," he says. Coinbase doesn't lend money, as banks do. And critically: Coinbase, which is regulated as a money transmitter like PayPal or Western Union, isn't covered by the FDIC or bound by all the consumer protection laws that govern banks.

Armstrong has long taken 100% of his salary in Bitcoin; he now cashes out enough into dollars each month to cover his rent. Many of his employees do the same. They understand the security issues better than just about anyone, yet protecting

customers is proving to be a gnarly challenge: Technically, because hackers are breaching accounts from the consumer end, exploiting weaknesses at companies like Verizon and Sprint, the hacks aren't directly Coinbase's fault. "Within the realm of reason, it's very difficult for us to prevent their account from being drained," says one executive.

Still, Coinbase can't afford to ignore the problem—literally. Even though it is not a bank, Coinbase still bears the cost of banking-system protocols, when traditional financial institutions yank back fraudulent payments induced by hackers. For example, when Dachis was robbed, a Coinbase customer support rep complained right back to him by email that "Coinbase has suffered a $1,657.41 USD loss due to bank reversals" of transactions subsequently reported as fraud. "Coinbase is left holding the bag," Soups Ranjan, the company's head of data science, said at a recent industry event. Problems like this—along with unauthorized credit card purchases of cryptocurrency—cost Coinbase a stunning 10% of all revenue it collects, a fraud-loss rate 20 times as high as PayPal's. "I firmly believe," Ranjan added, "we have the hardest payment fraud and user security problem in the world right now."

To combat that, Coinbase has been using analytics to predict which customers have the highest risk of fraud and charge-backs, and preemptively limiting their purchasing power or locking their accounts. But that method comes with a downside of its own in the form of frustrated customers—and a backlog of help-desk requests that has stretched into the tens of thousands. With about 180 employees, the company hasn't been able to hire fast enough to keep up with demand and is now looking to fill another 100 positions. Coinbase doesn't even have a phone number for customer support, though it plans to add one in September.

At the same time, Coinbase finds itself slamming headfirst into the expectations that come with being the closest thing cryptocurrency has to Goldman Sachs. The IRS has gone to court seeking Coinbase user records, after only 802 U.S. taxpayers reported Bitcoin profits on their tax returns in 2015. In June, Coinbase had its first "flash crash," with Ethereum's price collapsing to 10¢ for a brief, panicky stretch; the company said that all trades "were executed properly" but eventually agreed, as a courtesy, to reimburse traders who had lost money owing to margin calls. And in early August, when a "hard fork" of the Bitcoin blockchain created another currency

called Bitcoin Cash, Coinbase initially said it wouldn't support it. Hours later, a denial-of-service cyberattack—which some perceived as retaliation—knocked the exchange completely offline, and customers began threatening to sue. Coinbase gave in: Account holders will be able to withdraw their Bitcoin Cash by 2018. "We're in a period of hypergrowth, and it's superexciting and a little chaotic," Armstrong says.

For many blockchain enthusiasts, the Coinbase hacks have been a reminder of the danger of letting anyone else store your cryptocurrency. "If you don't own the private keys, you don't own the coin," says Jonathan Smith, the chief technology officer of Civic, a company that uses blockchain tech for identity verification. Then again, Bitcoin has a dirty little secret: For an asset that epitomizes the future, managing your coin yourself can feel like a journey into the troglodytic past.

Smart-money investors who store their own keys often resort to the most rudimentary of tactics to protect them. They're the Bitcoin equivalent of stuffing cash under the mattress: a private key printed out on a sheet of paper, cut into pieces, and distributed among family members who don't know how to put it back together; an encrypted file loaded on a USB stick and buried in the backyard; a password committed only to memory. These jury-rigged methods come with their own pitfalls, and stories of self-inflicted losses are legion: The New York man who reformatted a hard drive and erased the key to $25,000 in Bitcoin. Dominic Fogarty, a hedge fund research analyst who left his phone, storing his cryptocurrency, in a taxi after a bachelor party—then schlepped all over the Adirondacks to retrieve it. ("Yes, we missed our train, but more importantly I didn't lose my Bitcoins!" he tells *Fortune*.)

The ultimate irony is that the gold standard in security, storing private keys in what's known as "cold storage," without connection to the Internet, often means putting them in the very places blockchain advocates hoped to avoid: banks. One cryptocurrency hedge fund manager once went to check on his safe-deposit box at Wells Fargo, which stored the key to $5 million, only to find the drawer empty. (A few weeks later, the correct box was found one slot below where it was supposed to be.) Even Coinbase itself relies on banks for some of its cold storage, where 98% of customer funds are kept. "It does seem a little old-fashioned, I suppose," Armstrong acknowledges. And yet, it may also be the future, as more mainstream investors want in on cryptocurrency but without the worries of BYOB.

For some crypto devotees, this is nothing less than heresy. Says Michael Krieger, a former Lehman Brothers analyst who abandoned Wall Street for cryptocurrency after becoming disillusioned by the financial crisis, "I wouldn't trust my crypto private keys to a safety-deposit box at a bank. That's just me." But already, the walls between finance's old guard and blockchain's renegades are beginning to crumble, and a day may come where the systems meld together almost seamlessly. "It's almost ironic and funny that some of the rules and procedures we want to get rid of are almost exactly the rules we want in place to [protect] a major client," says Hu Liang, a former State Street exec who left in August to start a cryptocurrency trading platform for institutional investors. Even as they dream of supplanting the conventions that have defined banking for centuries, blockchain disciples are realizing that you can never quite escape them.

Jonathan Levin is still catching his breath from a six-mile bike commute as he welcomes me into his office, on the second floor of a Manhattan coworking space, early one August morning. Wearing a gray cotton T-shirt that reads "Bitcoin, est. 2009," the 27-year-old British expat exclaims cheekily, "So this is what fighting cybercrime looks like!"

Levin is the cofounder of Chainalysis, a startup that tracks virtual currency movement and investigates illicit use. Chainalysis's software assisted law enforcement with the takedowns and criminal indictments of both "dark net" marketplace AlphaBay and notorious digital currency exchange BTC-e during the span of a week in July, according to people familiar with the investigations. Previously, the company was able to locate where the stolen money from Mt. Gox and Bitfinex ended up: Bitcoin keeps an immutable record of all transactions—a literal money trail—so anyone can see the addresses of the digital wallets where funds are sent. Chainalysis's artificial intelligence "clustering" techniques mapped the funds to particular exchanges. But progress seems to have hit a dead end when it comes to determining who controls those wallets. "How many people have been caught for stealing money from major Bitcoin exchanges?" Levin asks rhetorically. "The answer is zero."

That's not entirely true, says Kathryn Haun, a former federal prosecutor who led the crackdown on virtual-currency crime and joined Coinbase's board in May. While no

one yet has gone to jail for hacking into an exchange or electronically pilfering cryptocurrency, she says, the AlphaBay and BTC-e probes are the first of a wave of cases that have yet to be completed or unsealed. Because wallet addresses are pseudonymous, it can take years for investigators to link them to a person—gathering data gleaned from exchanges like Coinbase and more obscure corners of the Internet. "I liken it to more traditional crimes, like bank robberies," Haun says. "If he's wearing a disguise and has a wig and gloves, it makes it that much harder to capture the criminal. But that doesn't mean it's impossible."

Individual thefts may be too small on their own to merit a federal case, but as more victims report crimes to the FBI and other government agencies, there's more cause for hope. Chainalysis, for its part, opened a special investigations unit in July to take on personal cases after fielding pleas for help from hack victims. And experts believe the criminals who commit the robberies belong to sophisticated organizations with the technology and manpower to trawl social networks for mentions of cryptocurrency accounts—the kinds of resources that let them, say, call Verizon 28 times in 24 hours until they succeed in porting a phone number, as they did in the case of Adam Pokornicky, managing partner at hedge fund Cryptochain Capital. Efforts that ambitious inevitably leave traces, and from such clues a pattern can emerge. "Phone porting cases and schemes like it have captured the attention of law enforcement, so I would say, stay tuned," Haun says.

That said, even if the blockchain world's combined forces succeed in capturing cybercriminals, there's no guarantee that victims will get their money back. Some of the legal precedent for charging cryptocurrency hackers is still untested, and there are questions as to whether intangible assets can even be seized. For one, accessing the booty would require knowing the private key: "They could get the criminal, but the government can't force them to say where the gold is," says Jeffrey Berns, whose California law firm specializes in digital currency. In a system that prizes decentralization above all else, the creature comforts of banking may never exist. Adds Berns, "There is no consumer protection, and I'm not sure it can be built in."

Deep inside a mountain in Switzerland, down a 200-meter cave, a World War II military bunker now stores what is believed to be the largest repository of Bitcoins on the planet. In the wake of the Mt. Gox hack in 2014, Wences Casares, an

Argentinean tech entrepreneur, thought there was one solution to storing digital coins: Go underground.

His company Xapo now operates heavily guarded vaults, on five continents, some as far as a kilometer down into the earth. Each contains so-called air-gapped servers on which the encrypted private keys are stored. To ensure hackers cannot rob its clients, who range from $5 account holders in emerging markets to the world's largest hedge funds and institutions, agents of Palo Alto–based Xapo personally witness the manufacturing of the servers before they even come off the assembly line and escort them to the hermetic vaults, guaranteeing they never touch the Internet. "It's somewhat ridiculous," says Casares, who also sits on the board of PayPal, "the extent to which we have to go to make sure that the keys are protected."

But even that safeguard has its limits. When customers move funds into a "hot wallet" on Xapo for transaction purposes (itself a 48-hour process), the money could be vulnerable to the same hacks that Coinbase accounts are. In other words, your cryptowealth is as safe as can be—until you want to actually use it.

Anatomy of a Cryptoheist

Coinbase account holders lose up to $5 million annually to theft by hacking, according to a person close to the company. Here's how the hacks happen, and why the culprits are so hard to catch.

The Stakeout

A scammer scouts a target by searching for people who work in the blockchain industry—or by combing social media for mentions of Bitcoin and Coinbase. The attacker finds the target's email address and phone number through online postings or previous
data leaks.

The Switcheroo

The scammer contacts the victim's mobile provider and "ports" the phone number to a device under the scammer's control.

The Disguise

Because Gmail accounts often link phone numbers as a backup access method, the scammer can now log in and reset the target's email password, then do the same at Coinbase.

"I'm In!"

Coinbase requires two-factor authentication ("2FA") in addition to a password. That 2FA now gets texted to the thief, who logs in.

The Getaway

The scammer moves the money into digital "wallets" under his control. Law enforcement can easily track the movements of the stolen currency recorded on the blockchain, but they can't block transactions, and figuring out who controls the wallets is difficult.

The Laundering

To try to cover his trail, the scammer can move the currency to foreign "cryptoexchanges," or convert it to other kinds of digital currency that are harder to track. Eventually, he can convert it to cash or other assets.

Building a Better Vault

For better security:

- Put a "do not port" order on your phone number.
- Don't use text-message 2FA; instead, use an app like Google Authenticator.
- Use a unique password, one you don't use for other accounts or social media.

This is part of *Fortune's* new initiative, *The Ledger,* a trusted news source at the intersection of tech and finance. For more on *The Ledger,* click here.

A version of this article appears in the Sept. 1, 2017 issue of Fortune with the headline "The 21st-Century Bank Robbery."